

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-257

Vulnerability Summary for the Week of September 7, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Unspecified vulnerability in the AClient agent in Symantec Altiris Deployment Solution 6.9.x before 6.9 SP3 Build 430, when key-based authentication is being used between a deployment server and a client, allows remote attackers to bypass authentication and execute arbitrary commands as SYSTEM by spoofing the deployment server and sending "alternate commands" before the handshake is completed.	2009-09-08	9.3	CVE-2009-3109 CONFIRM BID
adium -- adium	Unspecified vulnerability in Adium before 1.2 has unknown impact and attack vectors related to javascript: URLs, possibly cross-site scripting (XSS).	2009-09-09	10.0	CVE-2008-7190 CONFIRM
adobe -- robohelp_server	Unspecified vulnerability in Adobe RoboHelp Server 8 might allow remote attackers to execute arbitrary code via unknown vectors, as demonstrated by the vd_adobe module in VulnDisco Pack Professional 8.7 through 8.11, related to a "remote pre-authentication exploit."	2009-09-04	10.0	CVE-2009-3068 BID MISC MISC MISC MISC SECUNIA MISC MISC
adobehp -- phppns	Multiple unspecified vulnerabilities in phppns before	2009-09-	10.0	CVE-2008-7198

auecwn -- phpms	2.1.1beta1 have unknown impact and attack vectors.	10	10.0	OSVDB MLIST
almondsoft -- com_aclassf	SQL injection vulnerability in the Almond Classifieds (com_aclassf) component 7.5 for Joomla! allows remote attackers to execute arbitrary SQL commands via the replid parameter in a manw_repl add_form action to index.php, a different vector than CVE-2009-2567.	2009-09-10	7.5	CVE-2009-3154 MILWoRM SECUNIA
apache -- http_server	The mod_proxy_ftp module in the Apache HTTP Server allows remote attackers to bypass intended access restrictions and send arbitrary commands to an FTP server via vectors related to the embedding of these commands in the Authorization HTTP header, as demonstrated by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	7.5	CVE-2009-3095 MISC
apple -- quicktime	Apple QuickTime before 7.6.4 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted H.264 movie file.	2009-09-10	9.3	CVE-2009-2202 BID CONFIRM APPLE
apple -- quicktime	Buffer overflow in Apple QuickTime before 7.6.4 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted MPEG-4 video file.	2009-09-10	9.3	CVE-2009-2203 BID CONFIRM APPLE
apple -- iphone_os	Multiple heap-based buffer overflows in the CoreAudio component in Apple iPhone OS before 3.1, and iPhone OS before 3.1.1 for iPod touch, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted (1) AAC or (2) MP3 file.	2009-09-10	9.3	CVE-2009-2206 CONFIRM APPLE
apple -- quicktime	Heap-based buffer overflow in Apple QuickTime before 7.6.4 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted FlashPix file.	2009-09-10	10.0	CVE-2009-2798 APPLE
apple -- quicktime	Heap-based buffer overflow in Apple QuickTime before 7.6.4 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted H.264 movie file.	2009-09-10	9.3	CVE-2009-2799 APPLE
apple -- iphone_os	The Telephony component in Apple iPhone OS before 3.1 does not properly handle SMS arrival notifications, which allows remote attackers to cause a denial of service (NULL pointer dereference and service interruption) via a crafted SMS message.	2009-09-10	7.8	CVE-2009-2815 CONFIRM SECUNIA APPLE
asterisk -- asterisk asterisk -- open_source asterisk -- opensource asterisk -- appliance_s800i	The IAX2 protocol implementation in Asterisk Open Source 1.2.x before 1.2.35, 1.4.x before 1.4.26.2, 1.6.0.x before 1.6.0.15, and 1.6.1.x before 1.6.1.6; Business Edition B.x.x before B.2.5.10, C.2.x before C.2.4.3, and C.3.x before C.3.1.1; and s800i 1.3.x before 1.3.0.3 allows remote attackers to cause a denial of service (call-number exhaustion) by initiating many IAX2 message exchanges, a related issue to CVE-2008-3263.	2009-09-08	7.8	CVE-2009-2346 BID BUGTRAQ SECTRACK SECUNIA CONFIRM

asus -- asus_wl-330ge	Unspecified vulnerability on the ASUS WL-330gE has unknown impact and remote attack vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	10.0	CVE-2009-3091 MISC
asus -- asus_wl-500w	Buffer overflow on the ASUS WL-500W wireless router has unknown impact and remote attack vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	10.0	CVE-2009-3092 BID SECUNIA MISC
asus -- asus_wl-500w	Unspecified vulnerability on the ASUS WL-500W wireless router has unknown impact and remote attack vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	10.0	CVE-2009-3093 BID SECUNIA MISC
bastian_blumentritt -- local_media_browser	Multiple unspecified vulnerabilities in Local Media Browser before 0.1 have unknown impact and attack vectors related to "Security holes."	2009-09-09	10.0	CVE-2008-7189 OSVDB CONFIRM MLIST
butterflymedia -- butterfly_organizer	Butterfly Organizer 2.0.0 allows remote attackers to (1) delete arbitrary categories via a modified tablehere parameter to category-delete.php with the is_js_confirmed parameter set to 1, or (2) delete arbitrary accounts via the mytable parameter to delete.php.	2009-09-08	7.5	CVE-2008-7181 XF BID MILWORM
carsten_wulff -- simplephpweb	admin/files.php in simplePHPWeb 0.2 does not require authentication, which allows remote attackers to perform unspecified administrative actions via unknown vectors. NOTE: some of these details are obtained from third party information.	2009-09-10	7.5	CVE-2009-3158 XF VUPEN MILWORM
cisco -- nexus_5000 cisco -- nexus_7000 cisco -- nx-os	Unspecified vulnerability in Cisco NX-OS before 4.0(1a)N2(1), when running on Nexus 5000 platforms, allows remote attackers to cause a denial of service (crash) via an unspecified "sequence of TCP packets" related to "TCP State manipulation," possibly related to separate attacks against CVE-2008-4609.	2009-09-08	7.8	CVE-2009-0627 CISCO
clip-share -- clipshare	ClipShare 2.6 does not properly restrict access to certain functionality, which allows remote attackers to change the profile of arbitrary users via a modified uid variable to siteadmin/useredit.php. NOTE: this can be used to recover the password of the user by using the modified e-mail address in the email parameter to recoverpass.php.	2009-09-09	7.5	CVE-2008-7188 XF BID MILWORM SECUNIA
danneo -- cms	SQL injection vulnerability in mod/poll/comment.php in the vote module in Danneo CMS 0.5.2 and earlier allows remote attackers to execute arbitrary SQL commands via the comtext parameter, in conjunction	2009-09-~~	7.5	CVE-2009-3118 VUPEN

	with crafted comname and comtitle parameters, in a poll action to index.php, related to incorrect input sanitization in base/danneo.function.php.	'9		SECUNIA MISC
deliantra -- deliantra	Double free vulnerability in Deliantra server engine before 2.4 has unknown impact and attack vectors.	2009-09-10	10.0	CVE-2008-7200 OSVDB CONFIRM
devscripts-devel_team -- devscripts	Eval injection vulnerability in scripts/uscan.pl before Rev 1984 in devscripts allows remote attackers to execute arbitrary Perl code via crafted pathnames on distribution servers for upstream source code used in Debian GNU/Linux packages.	2009-09-04	9.3	CVE-2009-2946 DEBIAN CONFIRM CONFIRM CONFIRM
evacms -- eva_cms	PHP remote file inclusion vulnerability in eva/index.php in EVA CMS 2.3.1, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the eva[caminho] parameter to index.php.	2009-09-08	8.5	CVE-2008-7183 XF BID MISC
fortinet -- fortigate-1000	Fortinet FortiGuard FortiGate-1000 3.00 build 040075,070111 allows remote attackers to bypass URL filtering via fragmented GET or POST requests that use HTTP/1.0 without the Host header. NOTE: this issue might be related to CVE-2005-3058.	2009-09-04	7.5	CVE-2008-7161 XF BID BUGTRAQ BUGTRAQ
g15tools -- g15daemon	Multiple unspecified vulnerabilities in G15Daemon before 1.9.4 have unknown impact and attack vectors.	2009-09-10	10.0	CVE-2008-7197 OSVDB MLIST
gameservers -- gsc	GSC build 2067 and earlier relies on the client to enforce administrator privileges, which allows remote attackers to execute arbitrary administrator commands via a crafted packet.	2009-09-08	10.0	CVE-2008-7170 XF BID BUGTRAQ
hp -- performance_insight	Multiple unspecified vulnerabilities in HP Performance Insight 5.3 allow remote attackers to have an unknown impact, related to (1) a "Remote exploit" on Windows platforms, and (2) a "Remote preauthentication exploit" on the Windows Server 2003 SP2 platform, as demonstrated by certain modules in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	10.0	CVE-2009-3096 SECUNIA MISC
hp -- performance_insight	Multiple unspecified vulnerabilities in HP Performance Insight 5.3 on Windows allow attackers to obtain sensitive information via unknown vectors, as demonstrated by certain modules in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	7.8	CVE-2009-3097 SECUNIA MISC
	Unspecified vulnerability in the Portal in HP Operations Dashboard 2.1 on Windows Server 2003 SP2 allows remote attackers to have an unknown impact, related to a "Remote exploit," as demonstrated			CVE-2009-

hp -- operations_dashboard	by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	10.0	3098 SECUNIA MISC
hp -- operations_manager	Unspecified vulnerability in HP OpenView Operations Manager 8.1 on Windows Server 2003 SP2 allows remote attackers to have an unknown impact, related to a "Remote exploit," as demonstrated by a certain module in VulnDisco Pack Professional 8.11, a different vulnerability than CVE-2007-3872. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	10.0	CVE-2009-3099 SECUNIA MISC
ibm -- tivoli_directory_server	IBM Tivoli Directory Server (TDS) 6.0 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via unspecified vectors, related to (1) the ibmslapd.exe daemon on Windows and (2) the ibmdiradm daemon in the administration server on Linux, as demonstrated by certain modules in VulnDisco Pack Professional 8.11, a different vulnerability than CVE-2006-0717. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	7.8	CVE-2009-3089 SECUNIA MISC
ibm -- lotus_notes	The RSS reader widget in IBM Lotus Notes 8.5 saves items from an RSS feed as local HTML documents, which allows remote attackers to execute arbitrary script in Internet Explorer's Local Machine Zone via a crafted feed.	2009-09-09	7.5	CVE-2009-3114 BID BUGTRAQ MISC
ibm -- websphere_mq	Unspecified vulnerability in the rriDecompress function in IBM WebSphere MQ 7.0.0.0, 7.0.0.1, and 7.0.0.2 allows remote attackers to cause a denial of service via unknown vectors.	2009-09-10	7.8	CVE-2009-3159 VUPEN AIXAPAR CONFIRM
ibm -- websphere_mq	IBM WebSphere MQ 6.x through 6.0.2.7, 7.0.0.0, 7.0.0.1, 7.0.0.2, and 7.0.1.0, when read ahead or asynchronous message consumption is enabled, allows attackers to have an unspecified impact via unknown vectors, related to a "memory overwrite" issue.	2009-09-10	8.8	CVE-2009-3160 VUPEN AIXAPAR CONFIRM
ibm -- websphere_mq	The server in IBM WebSphere MQ 7.0.0.1, 7.0.0.2, and 7.0.1.0 allows attackers to cause a denial of service (trap) or possibly have unspecified other impact via malformed data.	2009-09-10	7.8	CVE-2009-3161 AIXAPAR CONFIRM
insane_visions -- onecms	Unrestricted file upload vulnerability in the add2 action in a_upload.php in OneCMS 2.4, and possibly earlier, allows remote attackers to execute arbitrary code by uploading a file with an executable extension and using a safe content type such as image/gif, then accessing it via a direct request to the file in an unspecified directory.	2009-09-11	7.5	CVE-2008-7209 BUGTRAQ
jabode -- com_jabode	SQL injection vulnerability in Jabode horoscope extension (com_jabode) for Joomla! allows remote attackers to execute arbitrary SQL commands via the id	2009-09-08	7.5	CVE-2008-7169 BID

	parameter in a sign task to index.php.			MILWORM
juracapecoffee -- internet_connectivity_kit	The Jura Internet Connection Kit for the Jura Impressa F90 coffee maker does not properly restrict access to privileged functions, which allows remote attackers to cause a denial of service (physical damage), modify coffee settings, and possibly execute code via a crafted request. NOTE: this issue is being included in CVE because the denial of service may include financial loss or water damage.	2009-09-08	10.0	CVE-2008-7173 BID BUGTRAQ BUGTRAQ BUGTRAQ OSVDB MISC VIM
juracapecoffee -- internet_connectivity_kit	Multiple buffer overflows in the Jura Internet Connection Kit for the Jura Impressa F90 coffee maker allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors related to improper use of the gets and sprintf functions.	2009-09-08	10.0	CVE-2008-7174 BID BUGTRAQ BUGTRAQ MISC
kde -- kdelibs	KDE KSSL in kdelibs 3.5.4, 4.2.4, and 4.3 does not properly handle a '\o' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-09-08	7.5	CVE-2009-2702 CONFIRM VUPEN SECUNIA
lantronix -- mss485-t	Lantronix MSS485-T allows remote attackers to cause a denial of service (unstable performance and service loss) via certain vulnerability scans, as demonstrated using (1) Nessus and (2) nmap.	2009-09-10	7.8	CVE-2008-7201 OSVDB FULLDISC
mark_reinsfelder -- metashell	Unspecified vulnerability in metashell before 0.03 has unknown impact and attack vectors related to a "PATH execution security flaw," possibly an untrusted search path vulnerability.	2009-09-10	10.0	CVE-2008-7196 OSVDB MLIST
microsoft -- windows_server_2008 microsoft -- windows_vista	Heap-based buffer overflow in the Wireless LAN AutoConfig Service (aka Wlansvc) in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a malformed wireless frame, aka "Wireless Frame Parsing Remote Code Execution Vulnerability."	2009-09-08	9.3	CVE-2009-1132 MS
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The JScript scripting engine 5.1, 5.6, 5.7, and 5.8 in JScript.dll in Microsoft Windows, as used in Internet Explorer, does not properly load decoded scripts into memory before execution, which allows remote attackers to execute arbitrary code via a crafted web site that triggers memory corruption, aka "JScript Remote Code Execution Vulnerability."	2009-09-08	9.3	CVE-2009-1920 MS
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista	The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 does not properly manage state information, which allows remote attackers to execute arbitrary code by sending packets to a listening service, and thereby triggering misinterpretation of an unspecified field as a function pointer, aka "TCP/IP Timestamps Code Execution Vulnerability."	2009-09-08	10.0	CVE-2009-1925 MS
microsoft -- windows_server_2003	Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allow remote attackers to cause a denial of service (TCP outage) via a series of TCP sessions that	2009-09-	~ 0	CVE-2009-1926

microsoft -- windows_server_2008 microsoft -- windows_vista	have pending data and a (1) small or (2) zero receive window size, and remain in the FIN-WAIT-1 or FIN-WAIT-2 state indefinitely, aka "TCP/IP Orphaned Connections Vulnerability."	08	1.0	1920 MS
microsoft -- media_foundation_sdk microsoft -- windows_media_format_runtime microsoft -- windows_media_services microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Windows Media Format Runtime 9.0, 9.5, and 11 and Windows Media Services 9.1 and 2008 do not properly parse malformed headers in Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted (1) .asf, (2) .wmv, or (3) .wma file, aka "Windows Media Header Parsing Invalid Free Vulnerability."	2009-09-08	9.3	CVE-2009-2498 MS
microsoft -- windows_media_format_runtime microsoft -- windows_media_foundation microsoft -- windows_media_services microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Windows Media Format Runtime 9.0, 9.5, and 11; and Microsoft Media Foundation on Windows Vista Gold, SP1, and SP2 and Server 2008; allows remote attackers to execute arbitrary code via an MP3 file with crafted metadata that triggers memory corruption, aka "Windows Media Playback Memory Corruption Vulnerability."	2009-09-08	9.3	CVE-2009-2499 MS
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_xp	The DHTML Editing Component ActiveX control in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly format HTML markup, which allows remote attackers to execute arbitrary code via a crafted web site that triggers "system state" corruption, aka "DHTML Editing Component ActiveX Control Vulnerability."	2009-09-08	9.3	CVE-2009-2519 MS
microsoft -- windows microsoft -- windows_server_2008 microsoft -- windows_vista	Array index error in the SMB2 protocol implementation in srv2.sys in Microsoft Windows 7, Server 2008, and Vista Gold, SP1, and SP2 allows remote attackers to cause a denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location. NOTE: some of these details are obtained from third party information.	2009-09-08	7.8	CVE-2009-3103 BID SECUNIA MISC MISC FULLDISC
mozilla -- firefox	Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-09-10	10.0	CVE-2009-3069 CONFIRM CONFIRM SECUNIA
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-09-10	10.0	CVE-2009-3070 CONFIRM CONFIRM CONFIRM CONFIRM

				SECUNIA
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.2, allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-09-10	10.0	CVE-2009-3071 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM SECUNIA
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.3, allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-09-10	10.0	CVE-2009-3072 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM SECUNIA
mozilla -- firefox	Unspecified vulnerability in the JavaScript engine in Mozilla Firefox 3.5.x before 3.5.3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-09-10	10.0	CVE-2009-3073 CONFIRM CONFIRM SECUNIA
mozilla -- firefox	Unspecified vulnerability in the JavaScript engine in Mozilla Firefox before 3.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-09-10	10.0	CVE-2009-3074 CONFIRM CONFIRM SECUNIA
mozilla -- firefox	Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.2, allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-09-10	10.0	CVE-2009-3075 CONFIRM CONFIRM CONFIRM SECUNIA
mozilla -- firefox	Mozilla Firefox before 3.0.14 does not properly implement certain dialogs associated with the (1) pkcs11.addmodule and (2) pkcs11.deletemodule operations, which makes it easier for remote attackers to trick a user into installing or removing an arbitrary PKCS11 module.	2009-09-10	9.3	CVE-2009-3076 CONFIRM CONFIRM SECUNIA
mozilla -- firefox	Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.3, does not properly manage pointers for the columns (aka TreeColumns) of a XUL tree element, which allows remote attackers to execute arbitrary code via a crafted HTML document, related to a "dangling pointer vulnerability."	2009-09-10	9.3	CVE-2009-3077 CONFIRM CONFIRM SECUNIA
mozilla -- firefox	Unspecified vulnerability in Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.3, allows remote attackers to execute arbitrary JavaScript with chrome privileges via vectors involving an object, the FeedWriter, and the BrowserFeedWriter.	2009-09-10	10.0	CVE-2009-3079 CONFIRM CONFIRM SECUNIA
multi-website -- multi_website	SQL injection vulnerability in index.php in Multi Website 1.5 allows remote attackers to execute arbitrary SQL commands via the Browse parameter in a vote action.	2009-09-10	7.5	CVE-2009-3150 VUPEN MILWoRM SECUNIA
				CVE-2008-7177 EEEDDAA

nasm -- nasm	Buffer overflow in the listing module in Netwide Assembler (NASM) before 2.03.01 has unknown impact and attack vectors, a different vulnerability than CVE-2008-2719.	2009-09-08	9.3	FEDORA CONFIRM VUPEN SECTRACK BID CONFIRM SECUNIA
openoffice -- openoffice.org	Unspecified vulnerability in OpenOffice.org (OOo) OpenOffice/Go-oo 2.x and 3.x allows remote attackers to execute arbitrary commands via a crafted EMF file.	2009-09-08	8.5	CVE-2009-2139 DEBIAN
otmanager -- otmanager_cms	OTManager CMS 2.4 allows remote attackers to bypass authentication and gain administrator privileges by setting the ADMIN_Hora, ADMIN_Logado, and ADMIN_Nome cookies to certain values, as reachable in Admin/index.php.	2009-09-08	7.5	CVE-2008-7179 BID MILWORM
oxidforge -- oxid_eshop oxidforge -- oxid_eshop4.0.0.2_14967	Unspecified vulnerability in OXID eShop Professional, Enterprise, and Community Edition before 4.1.0 allows remote attackers to gain administrator privileges and access the shop backend via a crafted parameter.	2009-09-09	10.0	CVE-2009-3112 CONFIRM
portalxp -- portalxp	Multiple SQL injection vulnerabilities in PortalXP Teacher Edition 1.2 allow remote attackers to execute arbitrary SQL commands via the id parameter to (1) calendar.php, (2) news.php, and (3) links.php; and the (4) assignment_id parameter to assignments.php.	2009-09-10	7.5	CVE-2009-3148 MILWORM
sami_ekblad -- page_manager	Unrestricted file upload vulnerability in upload.php in Page Manager 2006-02-04 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in an unspecified directory.	2009-09-08	10.0	CVE-2008-7167 XF VUPEN BID MILWORM
silcnet -- silc_client silcnet -- silc_toolkit	Multiple format string vulnerabilities in lib/silcclient/client_entry.c in Secure Internet Live Conferencing (SILC) Toolkit before 1.1.10, and SILC Client before 1.1.8, allow remote attackers to execute arbitrary code via format string specifiers in a nickname field, related to the (1) silc_client_add_client, (2) silc_client_update_client, and (3) silc_client_nickname_format functions.	2009-09-10	7.5	CVE-2009-3051 VUPEN BID DEBIAN CONFIRM CONFIRM
silcnet -- silc_client silcnet -- silc_toolkit	Multiple format string vulnerabilities in lib/silcclient/command.c in Secure Internet Live Conferencing (SILC) Toolkit before 1.1.10, and SILC Client 1.1.8 and earlier, allow remote attackers to execute arbitrary code via format string specifiers in a channel name, related to (1) silc_client_command_topic, (2) silc_client_command_kick, (3) silc_client_command_leave, and (4) silc_client_command_users.	2009-09-10	7.5	CVE-2009-3163 BID MLIST MLIST DEBIAN CONFIRM CONFIRM SECUNIA
snowhall -- silurus_system	SQL injection vulnerability in wcategory.php in Snow Hall Silurus System 1.0 allows remote attackers to execute arbitrary SQL commands via the ID parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-04	7.5	CVE-2009-3082 SECUNIA
snowhall -- silurus_system	SQL injection vulnerability in category.php in Snow Hall Silurus System 1.0 allows remote attackers to	2009-09-08	7.5	CVE-2009-3117 XF K7GWDDN

	execute arbitrary SQL commands via the ID parameter.	99	VUPEN MILWORM SECUNIA
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the IPv6 networking stack in Sun Solaris 10, and OpenSolaris snv_01 through snv_82 and snv_111 through snv_122, when a Cassini GigaSwift Ethernet Adapter (aka CE) interface is used, allows remote attackers to cause a denial of service (panic) via vectors involving jumbo frames. NOTE: this issue exists because of an incomplete fix for CVE-2009-2136.	2009-09-10	7.1 CVE-2009-3164 CONFIRM
symantec -- altiris_deployment_solution	The Aclient GUI in Symantec Altiris Deployment Solution 6.9.x before 6.9 SP3 Build 430 installs a client executable with insecure permissions (Everyone:Full Control), which allows local users to gain privileges by replacing the executable with a Trojan horse program.	2009-09-08	7.2 CVE-2009-3108 CONFIRM SECTRACK BID SECUNIA
uiga -- church_portal	SQL injection vulnerability in index.php in Uiga Church Portal allows remote attackers to execute arbitrary SQL commands via the month parameter in a calendar action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-04	7.5 CVE-2009-3081 XF SECUNIA OSVDB
uiga -- church_portal	SQL injection vulnerability in index.php in Uiga Church Portal allows remote attackers to execute arbitrary SQL commands via the year parameter in a calendar action.	2009-09-09	7.5 CVE-2009-3116 XF VUPEN MILWORM SECUNIA OSVDB
uusee -- uusee uusee -- uuupgrade.ocx	Insecure method vulnerability in the UUSee UUUpgrade ActiveX control (UUUpgrade.ocx 3.0.2.12) allows remote attackers to force the download and overwrite of arbitrary files via crafted arguments to the Update method, as exploited in the wild in June 2009.	2009-09-08	9.3 CVE-2008-7168 XF BID MISC
vmware -- ace vmware -- movie_decoder vmware -- player vmware -- workstation	Heap-based buffer overflow in the VMnc media codec in vmnc.dll in VMware Movie Decoder before 6.5.3 build 185404, VMware Workstation 6.5.x before 6.5.3 build 185404, VMware Player 2.5.x before 2.5.3 build 185404, and VMware ACE 2.5.x before 2.5.3 build 185404 on Windows might allow remote attackers to execute arbitrary code via a video file with crafted dimensions (aka framebuffer parameters).	2009-09-08	9.3 CVE-2009-0199 VUPEN CONFIRM BID BUGTRAQ MLIST
vmware -- ace vmware -- movie_decoder vmware -- player vmware -- workstation	The VMnc media codec in vmnc.dll in VMware Movie Decoder before 6.5.3 build 185404, VMware Workstation 6.5.x before 6.5.3 build 185404, VMware Player 2.5.x before 2.5.3 build 185404, and VMware ACE 2.5.x before 2.5.3 build 185404 on Windows does not properly handle certain small heights in video content, which might allow remote attackers to execute arbitrary code via a crafted AVI file that triggers heap memory corruption.	2009-09-08	10.0 CVE-2009-2628 CERT-VN
x-iweb.ru -- download_system_msf	SQL injection vulnerability in screen.php in the Download System msf (dsmssf) module for PHP-Fusion allows remote attackers to execute arbitrary SQL commands via the view_id parameter.	2009-09-09	7.5 CVE-2009-3119 VUPEN BID MISC

xoops -- uploader	Directory traversal vulnerability in Uploader module 1.1 for XOOPS allows remote attackers to read arbitrary files via a .. (dot dot) in the filename parameter in a downloadfile action to index.php.	2009-09-08	7.5	CVE-2008-7178 XF BID MILWORM
yanick_bourbeau -- lightweight_news_portal	Lightweight news portal (LNP) 1.0b does not properly restrict access to administrator functionality, which allows remote attackers to gain administrator privileges via direct requests to admin.php with the (1) potd_delete, (2) potd, (3) vote_update, (4) vote, or (5) modifynews actions.	2009-09-08	7.5	CVE-2008-7172 XF BID MILWORM
zmanda -- zrm_for_my_sql	The doHotCopy subroutine in socket-server.pl in Zmanda Recovery Manager (ZRM) for MySQL 2.x before 2.1.1 allows remote attackers to execute arbitrary commands via vectors involving a crafted \$MYSQL_BINPATH variable.	2009-09-08	10.0	CVE-2009-3102 XF XF MISC MISC MISC SECUNIA SECUNIA MISC
zyxel -- p-330w_router	Multiple cross-site request forgery (CSRF) vulnerabilities in the web management interface in the ZyXEL P-330W router allow remote attackers to hijack the authentication of administrators for requests that (1) enable remote router management via goform/formRmtMgt or (2) modify the administrator password via goform/formPasswordSetup.	2009-09-10	9.3	CVE-2007-6730 SECUNIA FULLDISC

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alex_rabe -- nextgen_gallery	Cross-site scripting (XSS) vulnerability in wp-admin/admin.php in NextGEN Gallery 0.96 and earlier plugin for Wordpress allows remote attackers to inject arbitrary web script or HTML via the picture description field in a page edit action.	2009-09-08	4.3	CVE-2008-7175 BUGTRAQ OSVDB
alice -- gate2_plus_wi-fi	Cross-site request forgery in cp06_wifi_m_nocifr.cgi in the administrator panel in TELECOM ITALIA Alice Gate2 Plus Wi-Fi allows remote attackers to hijack the authentication of administrators for requests that disable Wi-Fi encryption via certain values for the wlChannel and wlRadioEnable parameters.	2009-09-04	6.8	CVE-2008-7165 XF BID BUGTRAQ SECUNIA OSVDB
allenthusiast -- reviewpost_php_pro	Cross-site scripting (XSS) vulnerability in showproduct.php in ReviewPost Pro vB3 allows remote attackers to inject arbitrary web script or HTML via the date parameter.	2009-09-10	4.3	CVE-2009-3147 OSVDB SECUNIA MISC
almondsoft -- com_aclassf	Cross-site scripting (XSS) vulnerability in gmap.php in the Almond Classifieds (com_aclassf) component 7.5 for Joomla! allows remote attackers to inject arbitrary web script or HTML via the addr parameter.	2009-09-10	4.3	CVE-2009-3155 OSVDB MILWORM SECUNIA
	Directory traversal vulnerability in index.php in			CVE-2009-3167

anantasoft -- gazelle_cms	Anantasoft Gazelle CMS 1.0, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the template parameter.	2009-09-11	4.3	BID MILWoRM MILWoRM SECUNIA
apache -- http_server	The ap_proxy_ftp_handler function in modules/proxy/proxy_ftp.c in the mod_proxy_ftp module in the Apache HTTP Server 2.0.63 and 2.2.13 allows remote FTP servers to cause a denial of service (NULL pointer dereference and child process crash) via a malformed reply to an EPSV command.	2009-09-08	5.4	CVE-2009-3094 MISC SECUNIA MISC
apple -- java_1.4 apple -- java_1.5 apple -- java_1.6 apple -- mac_os_x apple -- mac_os_x_server	Stack-based buffer overflow in the Java Web Start command launcher in Java for Mac OS X 10.5 before Update 5 allows attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.	2009-09-09	6.8	CVE-2009-2205 SECTRACK APPLE
apple -- iphone_os	The Exchange Support component in Apple iPhone OS before 3.1, and iPhone OS before 3.1.1 for iPod touch, does not properly implement the "Maximum inactivity time lock" functionality, which allows local users to bypass intended Microsoft Exchange restrictions by choosing a large Require Passcode time value.	2009-09-10	4.6	CVE-2009-2794 CONFIRM SECUNIA APPLE
apple -- iphone_os	Heap-based buffer overflow in the Recovery Mode component in Apple iPhone OS before 3.1, and iPhone OS before 3.1.1 for iPod touch, allows local users to bypass the passcode requirement and access arbitrary data via vectors related to "command parsing."	2009-09-10	4.9	CVE-2009-2795 CONFIRM SECUNIA APPLE
apple -- iphone_os	The WebKit component in Safari in Apple iPhone OS before 3.1, and iPhone OS before 3.1.1 for iPod touch, does not remove usernames and passwords from URLs sent in Referer headers, which allows remote attackers to obtain sensitive information by reading Referer logs on a web server.	2009-09-10	5.0	CVE-2009-2797 CONFIRM SECUNIA APPLE
apple -- mac_os_x apple -- mac_os_x_server	Buffer overflow in Alias Manager in Apple Mac OS X 10.4.11 and 10.5.8 allows attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted alias file.	2009-09-11	6.8	CVE-2009-2800 CONFIRM APPLE
articlefriend -- articlefriend_script	Cross-site scripting (XSS) vulnerability in search_advance.php in ArticleFriend Script allows remote attackers to inject arbitrary web script or HTML via the SearchWd parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-10	4.3	CVE-2009-3146 XF SECUNIA OSVDB
bigace -- bigace	Cross-site scripting (XSS) vulnerability in public/index.php in BIGACE Web CMS 2.6 allows remote attackers to inject arbitrary web script or HTML via the id parameter. NOTE: some of these details are obtained from third party information.	2009-09-09	4.3	CVE-2009-3120 CONFIRM
bittorrent -- bittorrent utorrent -- utorrent	Buffer overflow in the web interface in BitTorrent 6.0.1 (build 7859) and earlier, and uTorrent 1.7.6 (build 7859) and earlier, allows remote attackers to cause a denial of service (memory consumption and crash) via a crafted Range header. NOTE: this is probably a different vulnerability than CVE-2008-0071 and CVE-2008-0364.	2009-09-04	5.0	CVE-2008-7166 VUPEN VUPEN SECUNIA SECUNIA OSVDB OSVDB MISC

celina_jorge -- facil_cms	Multiple directory traversal vulnerabilities in Facil CMS 0.1RC allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) change_lang parameter to index.php or (2) modload parameter to modules.php.	2009-09-08	5.0	CVE-2009-7176 XF BID MILWORM
chris_shattuck -- ajaxtable	Cross-site scripting (XSS) vulnerability in the Ajax Table module 5.x for Drupal allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-09-09	4.3	CVE-2009-3121 CONFIRM
chris_shattuck -- ajaxtable	The Ajax Table module 5.x for Drupal does not perform access control, which allows remote attackers to delete arbitrary users and nodes via unspecified vectors.	2009-09-09	6.4	CVE-2009-3122 XF VUPEN BID OSVDB SECUNIA CONFIRM
cmu -- cyrus_imap_server	Buffer overflow in the SIEVE script component (sieve/script.c) in cyrus-imapd in Cyrus IMAP Server 2.2.13 and 2.3.14 allows local users to execute arbitrary code and read or modify arbitrary messages via a crafted SIEVE script, related to the incorrect use of the sizeof operator for determining buffer length, combined with an integer signedness error.	2009-09-08	4.4	CVE-2009-2632 VUPEN BID DEBIAN
coppermine-gallery -- coppermine_photo_gallery	Coppermine Photo Gallery (CPG) 1.4.14 does not restrict access to update.php, which allows remote attackers to obtain sensitive information such as the database table prefix via a direct request. NOTE: this might be leveraged for attacks against CVE-2008-0504.	2009-09-09	5.0	CVE-2008-7186 VUPEN
coppermine-gallery -- coppermine_photo_gallery	Coppermine Photo Gallery (CPG) 1.4.14 allows remote attackers to obtain sensitive information via a direct request to include/slideshow.inc.php, which leaks the installation path in an error message.	2009-09-09	5.0	CVE-2008-7187 VUPEN
diigo -- diigo_toolbar diigo -- diigolet	Cross-site scripting (XSS) vulnerability in Diigo Toolbar and Diigolet allows remote attackers to inject arbitrary web script or HTML via a public comment.	2009-09-08	4.3	CVE-2008-7184 XF BID BUGTRAQ
elgg -- elgg	Directory traversal vulnerability in _css/js.php in Elgg 1.5, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the js parameter. NOTE: some of these details are obtained from third party information.	2009-09-10	4.3	CVE-2009-3149 MILWORM SECUNIA
freeradius -- freeradius	The rad_decode function in FreeRADIUS before 1.1.8 allows remote attackers to cause a denial of service (radiusd crash) via zero-length Tunnel-Password attributes. NOTE: this is a regression error related to CVE-2003-0967.	2009-09-09	5.0	CVE-2009-3111 MLIST CONFIRM
fujitsu -- interstage_application_server	Unspecified vulnerability in Fujitsu Interstage HTTP Server, as used in Interstage Application Server 5.0, 7.0, 7.0.1, and 8.0.0 for Windows, allows attackers to cause a denial of service via a crafted request.	2009-09-10	5.0	CVE-2008-7194 CONFIRM
fujitsu -- interstage_application_server	Unspecified vulnerability in Fujitsu Interstage HTTP Server, as used in Interstage Application Server Enterprise Edition 7.0.1 for Solaris, allows attackers to cause a denial of service via unknown vectors related to SSL.	2009-09-10	5.0	CVE-2008-7195 VUPEN CONFIRM
	The Red Hat build script for the GNOME Display			CVE-2009-

gnome -- gdm	Manager (GDM) before 2.16.0-56 on Red Hat Enterprise Linux (RHEL) 5 omits TCP Wrapper support, which might allow remote attackers to bypass intended access restrictions via XDMCP connections, a different vulnerability than CVE-2007-5079.	2009-09-04	6.8	2697 REDHAT CONFIRM BID SECUNIA
gnome -- rhythmbox	GNOME Rhythmbox 0.11.5 allows remote attackers to cause a denial of service (segmentation fault and crash) via a playlist (.pls) file with a long Title field, possibly related to the g_hash_table_lookup function in b-playlist-manager.c.	2009-09-08	5.0	CVE-2008-7185 XF BID BUGTRAQ BUGTRAQ MISC
ibm -- lotus_domino	Unspecified vulnerability in nserver.exe in the server in IBM Lotus Domino 8.0 on Windows Server 2003 allows remote attackers to cause a denial of service (daemon crash) via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	5.0	CVE-2009-3087 SECUNIA MISC
ibm -- tivoli_directory_server	Heap-based buffer overflow in ibmdiradm in IBM Tivoli Directory Server (TDS) 6.0 on Linux allows remote attackers to have an unspecified impact via unknown vectors that trigger heap corruption, as demonstrated by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	5.0	CVE-2009-3088 SECUNIA MISC
ibm -- tivoli_directory_server	Unspecified vulnerability in IBM Tivoli Directory Server (TDS) 6.0 on Linux allows remote attackers to cause a denial of service via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-08	5.0	CVE-2009-3090 SECUNIA MISC
ibm -- domino_web_access	Cross-site scripting (XSS) vulnerability in IBM Lotus iNotes (aka Domino Web Access or DWA) before 211.241 for Domino 8.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka SPR EZEL7UURYC.	2009-09-08	4.3	CVE-2009-3105 VUPEN BID CONFIRM SECUNIA
ibm -- websphere_application_server	The Servlet Engine/Web Container component in IBM WebSphere Application Server (WAS) 6.0.2 before 6.0.2.37 does not properly implement security constraints on the (1) doGet and (2) doTrace methods, which allows remote attackers to bypass intended access restrictions and obtain sensitive information via a crafted HTTP HEAD request to a Web Application.	2009-09-08	5.0	CVE-2009-3106 CONFIRM
insane_visions -- onecms	Multiple SQL injection vulnerabilities in OneCMS 2.4, and possibly earlier, allow remote attackers to execute arbitrary SQL commands via the (1) username parameter (\$usernameb variable) to a_login.php or (2) user parameter to staff.php.	2009-09-11	6.8	CVE-2008-7208 CONFIRM
	Directory traversal vulnerability in get_message.cgi in	2009-09-11		CVE-2009-3104

ipmotor -- quarkmail	QuarkMail allows remote attackers to read arbitrary files via a .. (dot dot) in the tf parameter.	2009-09-09	5.0	3124 VUPEN MISC
mozilla -- firefox	Visual truncation vulnerability in Mozilla Firefox before 3.0.14, and 3.5.x before 3.5.3, allows remote attackers to trigger a vertical scroll and spoof URLs via unspecified Unicode characters with a tall line-height property.	2009-09-10	5.0	CVE-2009-3078 CONFIRM CONFIRM SECUNIA
multi-website -- multi_website	Cross-site scripting (XSS) vulnerability in Multi Website 1.5 allows remote attackers to inject arbitrary web script or HTML via the search parameter in a search action to the default URI.	2009-09-10	4.3	CVE-2009-3162 SECUNIA MISC
netwin -- surgemail	Buffer overflow in the IMAP service in NetWin Surgemail 3.9e, and possibly other versions before 3.9g2, allows remote authenticated users to cause a denial of service (crash) and possibly execute arbitrary code via a long first argument to the APPEND command, a different vector than CVE-2008-1497 and CVE-2008-1498. NOTE: due to lack of details, it is not certain whether this is the same issue as CVE-2008-2859.	2009-09-08	4.0	CVE-2008-7182 BID BUGTRAQ MISC MILWORM
nt -- bbs_e-market_professional	Multiple cross-site scripting (XSS) vulnerabilities in becommunity/community/index.php in NTSOFT BBS E-Market Professional allow remote attackers to inject arbitrary web script or HTML via the (1) page, (2) bt_code, and (3) b_no parameters in a board view action.	2009-09-10	4.3	CVE-2009-3152 XF BID SECUNIA MISC
openwebmail.acatysmoof -- openwebmail	Multiple cross-site scripting (XSS) vulnerabilities in OpenWebMail before 2.53 (Stable) allow remote attackers to inject arbitrary web script or HTML via unknown vectors.	2009-09-10	4.3	CVE-2008-7202 CONFIRM
oxid -- eshop	OXID eShop 4.x before 4.1.4-21266, 3.x, and 2.x allows remote attackers to obtain sensitive information (session details and order history of other users) via a crafted cookie.	2009-09-09	4.3	CVE-2009-2266 CONFIRM
oxid -- eshop	Unspecified vulnerability in OXID eShop Professional, Enterprise, and Community Edition before 4.1.2, 3.x, and 2.x allows remote attackers to gain write access to product reviews via a crafted parameter.	2009-09-09	5.0	CVE-2009-3113 CONFIRM
phoenixcontact -- fl_il_24_bk-pac	Phoenix Contact FL IL 24 BK-PAC allows remote attackers to cause a denial of service (hang) via (1) unspecified manipulations as demonstrated by a Nessus scan or (2) malformed input to TCP port 502.	2009-09-10	5.0	CVE-2008-7199 OSVDB FULLDISC
phpkit -- phplib	PHPKIT 1.6.4 PL1 includes the session ID in the URL, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks by reading the PHPKITSID parameter from the HTTP Referer and using it in a request to (1) modify the user profile via upload_files/include.php or (2) create a new administrator via upload_files/pk/include.php.	2009-09-09	6.8	CVE-2008-7193 XF BUGTRAQ OSVDB
pidgin -- libpurple pidgin -- pidgin	libpurple/protocols/irc/msgs.c in the IRC protocol plugin in libpurple in Pidgin before 2.6.2 allows remote IRC servers to cause a denial of service (NULL pointer dereference and application crash) via a TOPIC message that lacks a topic string.	2009-09-08	5.0	CVE-2009-2703 CONFIRM CONFIRM
	The msn_slp_sip_recv function in libpurple/protocols/msn/slpc in the MSN protocol plugin in libpurple in Pidgin before 2.6.2 allows remote			CVE-2009-3083

pidgin -- libpurple pidgin -- pidgin	attackers to cause a denial of service (NULL pointer dereference and application crash) via an SLP invite message that lacks certain required fields, as demonstrated by a malformed message from a KMess client.	2009-09-08	5.0	CONFIRM CONFIRM CONFIRM CONFIRM
pidgin -- libpurple pidgin -- pidgin	The msn_slp_process_msg function in libpurple/protocols/msn/slpcall.c in the MSN protocol plugin in libpurple 2.6.0 and 2.6.1, as used in Pidgin before 2.6.2, allows remote attackers to cause a denial of service (application crash) via a handwritten (aka Ink) message, related to an uninitialized variable and the incorrect "UTF16-LE" charset name.	2009-09-08	5.0	CVE-2009-3084 CONFIRM CONFIRM CONFIRM
pidgin -- libpurple pidgin -- pidgin	The XMPP protocol plugin in libpurple in Pidgin before 2.6.2 does not properly handle an error IQ stanza during an attempted fetch of a custom smiley, which allows remote attackers to cause a denial of service (application crash) via XHTML-IM content with cid: images.	2009-09-08	5.0	CVE-2009-3085 CONFIRM CONFIRM
pps.jussieu -- polipo	Unspecified vulnerability in Polipo before 1.0.4 allows remote attackers to cause a denial of service (crash) via a long request URL.	2009-09-09	5.0	CVE-2008-7191 CONFIRM OSVDB
ruby_on_rails -- ruby_on_rails	Cross-site scripting (XSS) vulnerability in Ruby on Rails 2.x before 2.2.3, and 2.3.x before 2.3.4, allows remote attackers to inject arbitrary web script or HTML by placing malformed Unicode strings into a form helper.	2009-09-08	4.3	CVE-2009-3009 VUPEN SECTRACK MLIST
ruby_on_rails -- ruby_on_rails	A certain algorithm in Ruby on Rails 2.1.0 through 2.2.2, and 2.3.x before 2.3.4, leaks information about the complexity of message-digest signature verification in the cookie store, which might allow remote attackers to forge a digest via multiple attempts.	2009-09-08	5.0	CVE-2009-3086 VUPEN CONFIRM
silcnet -- silc_toolkit	The silc_asn1_encoder function in lib/silcasn1/silcasn1_encode.c in Secure Internet Live Conferencing (SILC) Toolkit before 1.1.8 allows remote attackers to overwrite a stack location and possibly execute arbitrary code via a crafted OID value, related to incorrect use of a %lu format string.	2009-09-10	5.8	CVE-2008-7159 BID MLIST DEBIAN CONFIRM CONFIRM
silcnet -- silc_toolkit	The silc_http_server_parse function in lib/silchttp/silchtpserver.c in the internal HTTP server in silcd in Secure Internet Live Conferencing (SILC) Toolkit before 1.1.9 allows remote attackers to overwrite a stack location and possibly execute arbitrary code via a crafted Content-Length header, related to incorrect use of a %lu format string.	2009-09-10	5.8	CVE-2008-7160 BID DEBIAN CONFIRM CONFIRM
solarwinds -- tftp_server	SolarWinds TFTP Server 9.2.0.111 and earlier allows remote attackers to cause a denial of service (service stop) via a crafted Option Acknowledgement (OACK) request. NOTE: some of these details are obtained from third party information.	2009-09-09	5.0	CVE-2009-3115 BID MILWoRM SECUNIA
stefan_ritt -- elog_web_logbook	Unspecified vulnerability in Electronic Logbook (ELOG) before 2.7.2 has unknown impact and attack vectors when the "logbook contains HTML code," probably cross-site scripting (XSS).	2009-09-11	4.3	CVE-2008-7206 BID
	xscreensaver (aka Gnome-XScreenSaver) in Sun Solaris 10, and OpenSolaris snv_109 through snv_122, does not			CVE-2009-

sun -- opensolaris sun -- solaris	properly handle Trusted Extensions, which allows local users to cause a denial of service (CPU consumption and console hang) by locking the screen, related to a regression in certain Solaris and OpenSolaris patches.	2009-09-08	4.9	3101 SUNALERT CONFIRM
symantec -- antivirus symantec -- client_security symantec -- norton_antivirus	Unspecified vulnerability in Symantec Norton AntiVirus 2005 through 2008; Norton Internet Security 2005 through 2008; AntiVirus Corporate Edition 9.0 before MR7, 10.0, 10.1 before MR8, and 10.2 before MR3; and Client Security 2.0 before MR7, 3.0, and 3.1 before MR8; when Internet Email Scanning is installed and enabled, allows remote attackers to cause a denial of service (CPU consumption and persistent connection loss) via unknown attack vectors.	2009-09-08	4.3	CVE-2009-3104 XF VUPEN CONFIRM BID SECUNIA OSVDB
symantec -- altiris_deployment_solution	Symantec Altiris Deployment Solution 6.9.x before 6.9 SP3 Build 430 does not properly restrict access to the listening port for the DBManager service, which allows remote attackers to bypass authentication and modify tasks or the Altiris Database via a connection to this service.	2009-09-08	4.8	CVE-2009-3107 CONFIRM SECTRACK BID SECUNIA
symantec -- altiris_deployment_solution	Race condition in the file transfer functionality in Symantec Altiris Deployment Solution 6.9.x before 6.9 SP3 Build 430 allows remote attackers to read sensitive files and prevent client updates by connecting to the file transfer port before the expected client does.	2009-09-08	6.4	CVE-2009-3110 CONFIRM SECTRACK BID SECUNIA
telephone -- telephone_directory_2008	del_query1.php in Telephone Directory 2008 allows remote attackers to delete arbitrary contacts via a direct request with a modified id variable.	2009-09-08	5.0	CVE-2008-7180 XF MILWORM
ultrize -- timesheet	Directory traversal vulnerability in actions/downloadFile.php in Ultrize TimeSheet 1.2.2 allows remote attackers to read arbitrary files via a .. (dot dot) in the fileName parameter.	2009-09-10	5.0	CVE-2009-3151 XF MILWORM
valvesoftware -- counter-strike	Valve Software Half-Life Counter-Strike 1.6 allows remote attackers to cause a denial of service (crash) via multiple crafted login packets.	2009-09-11	5.0	CVE-2008-7203 XF BID MILWORM
virtuemart -- virtuemart	Cross-site request forgery (CSRF) vulnerability in VirtueMart 1.0.13a and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2009-09-11	6.8	CVE-2008-7204 CONFIRM
virtuemart -- virtuemart	Unspecified vulnerability in the product view functionality in VirtueMart 1.0.13a and earlier allows remote attackers to read arbitrary files via vectors related to a template file.	2009-09-11	4.3	CVE-2008-7205 BID CONFIRM
visavi -- wap-motor	Directory traversal vulnerability in gallery/gallery.php in Wap-Motor before 18.1 allows remote attackers to read arbitrary files via a .. (dot dot) in the image parameter.	2009-09-09	5.0	CVE-2009-3123 XF SECUNIA MISC OSVDB
woltlab -- burning_board	Cross-site request forgery (CSRF) vulnerability in index.php in WoltLab Burning Board (wBB) 3.0.1, and possibly other 3.x versions, allows remote attackers to hijack the authentication of users for requests that delete	2009-09-20	6.8	CVE-2008-7192 vF

	private messages via the pmID parameter in a delete action in a PM page, a different vulnerability than CVE-2008-0472.	09		 BUGTRAQ
x.org -- x11 sun -- opensolaris sun -- solaris	xscreensaver (aka Gnome-XScreenSaver) in Sun Solaris 9 and 10, OpenSolaris snv_109 through snv_122, and X11 6.4.1 on Solaris 8 does not properly handle Accessibility support, which allows local users to cause a denial of service (system hang) by locking the screen and then attempting to launch an Accessibility pop-up window, related to a regression in certain Solaris and OpenSolaris patches.	2009-09-08	4.0	CVE-2009-3100 SUNALERT
x10media -- mp3_search_engine	Multiple cross-site scripting (XSS) vulnerabilities in x10 MP3 Search engine 1.6.5 allow remote attackers to inject arbitrary web script or HTML via the (1) pic_id parameter to includes/video_ad.php, (2) category parameter to linkvideos_listing.php, id parameter to (3) templates/header1.php and (4) mp3/lyrics.php, key parameter to (5) video_listing.php and (6) adult/video_listing.php, and name parameter to (7) mp3/embed.php and (8) mp3/info.php.	2009-09-10	4.3	CVE-2009-3153 XF SECUNIA MISC
yanick_bourbeau -- lightweight_news_portal	Multiple cross-site scripting (XSS) vulnerabilities in Lightweight news portal (LNP) 1.0b allow remote attackers to inject arbitrary web script or HTML via the (1) photo parameter to show_photo.php, (2) potd parameter to show_potd.php, or (3) the Current question field in a vote action to admin.php.	2009-09-08	4.3	CVE-2008-7171 XF XF BID MILWORM
zope -- zodb	Unspecified vulnerability in the Zope Enterprise Objects (ZEO) storage-server functionality in Zope Object Database (ZODB) 3.8 before 3.8.3 and 3.9.x before 3.9.0c2, when certain ZEO database sharing and blob support are enabled, allows remote authenticated users to read or delete arbitrary files via unknown vectors.	2009-09-08	6.0	CVE-2009-2701 MLIST VUPEN CONFIRM CONFIRM
zyxel -- p-330w_router	Cross-site scripting (XSS) vulnerability in the web management interface in the ZyXEL P-330W router allows remote attackers to inject arbitrary web script or HTML via the pingstr parameter and other unspecified vectors.	2009-09-10	4.3	CVE-2007-6729 SECUNIA FULLDISC

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- iphone_os	The MobileMail component in Apple iPhone OS 3.0 and 3.0.1, and iPhone OS 3.0 for iPod touch, lists deleted e-mail messages in Spotlight search results, which might allow local users to obtain sensitive information by reading these messages.	2009-09-10	2.1	CVE-2009-2207 CONFIRM SECUNIA APPLE
apple -- iphone_os	The UIKit component in Apple iPhone OS 3.0, and iPhone OS 3.0.1 for iPod touch, allows physically proximate attackers to discover a password by watching a user undo deletions of characters in the password.	2009-09-10	2.1	CVE-2009-2796 CONFIRM SECUNIA APPLE
karen_stevenson -- date	Cross-site scripting (XSS) vulnerability in the Date Tools sub-module in the Date module 6.x before 6.x-2.3 for Drupal allows remote authenticated users, with "use date tools" or "administer content types" privileges, to inject	2009-09-10	3.5	CVE-2009-3156 CONFIRM

	arbitrary web script or HTML via a "Content type label" field.			CONFIRM
karen_stevenson -- calendar	Cross-site scripting (XSS) vulnerability in the Calendar module 6.x before 6.x-2.2 for Drupal allows remote authenticated users, with "create new content types" privileges, to inject arbitrary web script or HTML via the title of a content type.	2009-09-10	3.5	CVE-2009-3157 BID CONFIRM CONFIRM
rivetcode -- rivetracker	RivetTracker before 1.0 stores passwords in cleartext in config.php, which allows local users to discover passwords by reading config.php.	2009-09-11	2.1	CVE-2008-7207 CONFIRM

[Back to top](#)**Last updated September 14, 2009** [Print This Document](#)